CHAPTER 5
INFORMATION TECHNOLOGY SERVICES CONTROLS

INTRODUCTION

In accordance with Statements on Auditing Standards Numbers 78 and 94, issued by the American Institute of Certified Public Accountants (AICPA), the State Board of Accounts may review applicable computers that process accounting data. Consideration in the selection of the computer systems to be reviewed includes but is not limited to total dollars processed by the computer system the complexity of the processing, the availability of alternate sources for audit information, and the criticality of non-financial information processed. The Information Technology Services (ITS) controls reviewed will be based primarily on the Control Objectives for Information Technology and other publications of the Information Systems Audit and Control Association. Additional sources of information used in State Board of Accounts' ITS reviews include but are not limited to publications of the AICPA, the Institute of Internal Auditors, the Government Accountability Office, the Department of Defense, the National Computer Security Association, and hardware and software vendors.

Governmental units should have internal controls in effect which provide reasonable assurance regarding the reliability of financial information and records, effectiveness and efficiency of operations, proper execution of managements' objectives, and compliance with laws and regulations. Among other things, segregation of duties, safeguarding controls over cash and all other assets and all forms of information processing are necessary for proper internal control.

The following requirements have been established for all computer systems processing accounting information. In the event these requirements are not met by the computer environment of the accounting system, compensating manual controls must be implemented.

DISASTER RECOVERY

A written Disaster Recovery Plan is required to ensure that critical accounting information will be processed in the event of interruption of computer processing capability. The plan must be updated and tested annually or when significant modifications to computer hardware, software or application systems occur. One copy of the Plan must be retained off site.

BACK UP PROCESSING

All computer application programs and operating system software must be backed up on a periodic basis and after modification. Accounting information must be backed up on a periodic basis sufficient to allow restoration of the information in a timely manner. Periodically the back up media must be tested to assure restoration will occur accurately. One copy of the back up information must be retained off site.

PHYSICAL SECURITY

The computer system and the associated telecommunications equipment must be adequately protected from environmental damage including, but not limited to, fire, water, and physical damage by individuals. In addition, the computer must be protected from unauthorized access, terminals must be inoperable when not attended by an authorized employee, and terminals utilized to enter sensitive commands must not be positioned where unauthorized individuals may view the contents of the video display terminal.

LOGICAL SECURITY

Effective logical security prohibits unauthorized access and restricts the computerized resources each authorized user may utilize. Access to accounting information and processes must be controlled by operating system software and by the computerized accounting application through user identification codes (user IDs) and passwords. User IDs are unique identifiers assigned to each authorized user, which remain constant for that user. Passwords are confidential keywords associated with the user ID to provide verification of the user's identity. Each user must have a unique user ID and password which must not be shared. Passwords must meet the following criteria:

- Passwords must be changed every 30 days.
- Passwords must be a minimum of six (6) characters in length.
- Passwords must be a combination of alphabetic and numeric characters.
- Passwords may not be the same for a user ID as the last five (5) passwords used by this user ID.
- Individuals must assign their own passwords.
- Passwords must be encrypted while stored on the computer.

Additional Logical Security requirements include:

- Reporting of security definitions and user access rights to information must be available to, and easily understood by, Management and State Board of Account Field Examiners during the course of a regularly scheduled audit. These security definitions and user access rights must enforce adequate segregation of duties for the accounting system.
- Users other than System Administrators and Security Administrators must be prevented from accessing sensitive operating system commands.
- The number of System Administrators and Security Administrators must be limited.
- Computer programmers must not have update access to production accounting information.
- Users must not be allowed to be active on multiple terminals at the same time with the same user ID.
- User IDs must be deactivated after three unsuccessful attempts to sign on to the computer.
- For inactive terminals, the user must be automatically prevented from accessing the computer after 15 minutes of no activity until the user's password is entered.
- Users must be prevented from modifying or deleting operating system and computer program files.
- Users must be prevented from updating accounting information except through authorized transactions within the computerized accounting application system.
- User access rights must be eliminated or revised upon termination of employment and transfers of employee responsibility.

CHANGE CONTROLS

Changes to the accounting system's computer programs must be adequately controlled including the following requirements:

- Computer source (human readable) and load (machine readable) modules must be protected from unauthorized modification.
- Modifications to computer source code must occur in a test environment and not affect production source code.
- All modifications to computer source code must be adequately tested. Modifications must be approved by management.
- Individuals responsible for modifying computer source code in a test environment must be prevented from updating computer code in the production environment. Movement of computer source and load modules from the test to production environments must be completed by authorized employees not responsible for modification of computer source or load modules.

AUDIT TRAILS

The computerized accounting system must maintain electronic audit trails sufficient to trace all transactions from original source of entry into the system, through all system processing, and to the results produced by the system. The audit trails must also maintain sufficient information to trace all transactions from the final results produced by the system, through all system processing, and to the original source of entry into the system. Audit trials must also identify the user that processed the transaction or updated the information. These audit trails must be protected from modification and deletion.

INPUT CONTROLS

The computerized accounting system must provide input edits and controls to assure that information entered into the system is accurate, that all appropriate information is entered into the system, and that information is entered into the system only once. All information entered into the system must be authorized through effective manual or electronic controls. Transaction dates should be based upon system generated dates which cannot be modified by the user. If necessary, the system may provide an additional effective date of the transaction that is user controlled.

SEGREGATION OF DUTIES

Segregation of duties is the concept of having different people do different tasks within the organization. It provides the foundation of good internal control by assuring that no one individual has the capability to perpetuate and conceal errors or irregularities in the normal course of their authorized duties. Segregation of duties is achieved within information technology systems by appropriate assignment of security profiles that define the data the users can access and the functions that they can perform. Access must be restricted to the minimum required for the user to perform their job function. Access rights must be periodically reviewed and approved by management.

OUTPUT CONTROLS

The computerized accounting system must incorporate features that assure all accounting information is reported accurately and completely. Procedures must also exist to assure that only authorized individuals have access to computer generated output. All receipts or payments generated by the accounting system must include unique document identification numbers either preprinted on the form or printed on the form by the application system. If the numbers are printed on the form by the application system, adequate security must be implemented to prevent unauthorized modification of the number sequence. Preprinted receipt and check stock must not include preprinted signatures, must be securely stored, and usage must be logged and reconciled. If the report content can be modified via user selection of various criteria such as account codes, department codes, transaction codes, status codes, etc., the report heading should contain sufficient information regarding the selection criteria to allow another user to understand what information is being reported and recreate the report. All output reports must clearly indicate the effective dates of the information in addition to the report generation date. Output reports must have appropriate subtotals to allow reconcilement to other reports and to external documentation.

INTERFACE CONTROLS

Information generated in one computer application system and transferred to another computer application system must be accurate and complete. Both systems should generate reports documenting record counts and the dollar value totals of the information transferred to enable prompt identification of discrepancies.

INTERNAL PROCESSING

When written verification procedures and actual verification results must be provided to the State Board of Accounts' Field Examiners which document accurate calculating, summarizing, categorizing, and updating of accounting information on a periodic basis and after the modification of accounting system computer programs.

ERROR CORRECTION

Accounting information must not be modified by computer utility programs which are not contained in the accounting application system. The accounting application system must be supported by computerized and manual procedures to assure the following error correction controls are implemented:

- The type of error condition is recorded.
- The original transaction creating the error is retained within the system.
- A reversing transaction to eliminate the effect of the error is entered and retained within the system.
- The correct transaction is entered into the system and recorded.
- Management approval for error correction is documented.

PROGRAMMING DOCUMENTATION

Documentation must be available to the State Board of Accounts' Field Examiners which provide adequate information on the functions performed by each computer program, the definitions of all computer files and records utilized by the computer programs, and a description of the computer processing which relates each computer program to other computer programs to accomplish accounting functions. The documentation must be adequate for the Field Examiners to determine the accuracy of accounting processes by the computer.

OPERATIONS DOCUMENTATION

For each computerized accounting system, procedures must be adequately documented to ensure all processing and maintenance is performed. Examples include instructions, checklists, and logs to ensure:

- Daily, monthly and year-end processes are performed correctly and completely.
- Required reports are generated and balanced.
- Backups are completed successfully and cycled appropriately.
- Virus definitions are updated regularly.
- Security patches and upgrades are installed.

USER DOCUMENTATION

Written procedures must be available for all computerized accounting systems which provide instructions on the requirements for the approval of information prior to entry into the computer, as well as the accurate entry, processing, and reporting of information from the accounting system.

COMPUTER OUTPUT

Public records, financial statement information and supporting information generated through the computer system must be maintained in a manner that will allow access for audit and public inquiry on equipment of the governmental unit.

PURCHASE OF DATA PROCESSING HARDWARE and/or SOFTWARE

The following is a general outline of steps to follow when contemplating the purchase of data processing hardware and/or software. The State Board of Accounts has an Information Technology Section available to help answer questions about IT requirements.

Basic Questions

- Is this purchase cost effective?
- Are sufficient funds available to purchase desired hardware and software?
- What applications are needed? Payroll? Financial and Appropriation Ledger? Accounts Payable?
- What is the current and future volume of transactions to be processed per application?
- Are qualified personnel available to operate the new system? How will they be trained?
- How will software be maintained?
- Can the vendor provide a list of users as references?
- Where is hardware/software maintenance staff located?
- What services are provided by the vendor when the system is down? How long before these services are available?
- What are the estimated maintenance costs?
- What is the cost to upgrade the system in the future?
- If the source code is not purchased, the vendor must allow access to the source code by representatives of the State Board of Accounts.

Software

- The accounting application should provide extensive editing of data and change capability upon input and before a transaction is posted to an account, but no ability to change data after it is posted. If an error is discovered after the transaction is posted, a separate correcting transaction must be made.
- The system should be capable of exporting electronic files of transactions and other data.
- A detailed transaction history (similar to a manually posted ledger page) must be maintained supporting each account. At least the last twelve months of transactions must be accessible on-line. Additional transactional history must be retained back to the date of the last audit. This additional history must be retained on-line or otherwise archived and easily accessible by State Board of Accounts Field Examiners.
- Copyright restrictions and documentation of all programs should be reviewed before purchase.
- If purchased separately, software must be compatible with hardware.

Hardware

- If purchased separately, hardware must be compatible with software.
- The hardware should have expansion capability to meet possible additional applications and future growth.
- Review vendor service agreements carefully for cost and completeness.

Steps to Take Prior to Bidding

- Communicate with all potential in-house users to insure that their business process requirements for the system are fully understood and the system will meet their needs.

- Verify that the system will provide the same information as the forms prescribed by the State Board of Accounts and fulfill the State Board of Accounts' Information Technology Services Controls.

- Observe hardware and software in operation at other units within the state and discuss with their users possible problems and/or suggestions, particularly service and maintenance.

Other Requirements

- Provisions must be made to backup the operating system, application software, and the data files. A copy of the backup should be stored offsite. In addition, a Disaster Recovery Plan should be developed when the system is installed.

- Review temperature, humidity and dust control requirements at the computer location.

- Review insurance coverage for hardware, software and file reconstruction.

- Appropriate procedures should be used in implementing the new system. For example, control totals during conversion of data and a parallel processing period. The results of conversion testing and reconcilements should be retained for audit.

POSSIBLE APPLICATIONS

The following is a list of possible applications with generalized minimum requirements.

Basically, minimum output requirements in an IT environment are the same as the forms prescribed by the State Board of Accounts.

Payroll

- Properly authorized, edited and extended before input.

- Individual time, earnings and deduction records should be maintained for each employee.

- Year-to- date totals available.

- Generate monthly, quarterly and annual reports.

- Totals by department.

- Overtime kept separately.

- Generation of State and Federal reports such as: W-2's, WH-3's, 1099's, etc.

Purchase Orders

- Properly authorized, edited and extended before input.
- Reduce purchase order balance when claim paid.
- Adjust for partial paid claim.
- Adjust for change in purchase order.
- Update appropriation ledger for encumbrances and payments.
- Update vendor record if applicable.